Data Network Resource

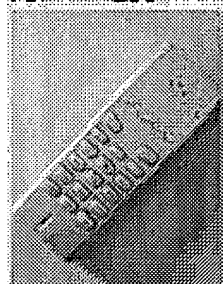| Physical Layer	Data Link Layer	Network Layer	Upper Layers	Misce

IP Addressin

Introduction

This section looks at IP addressing, subnet masking, Private and Spec
illustrate the methodology when setting up an IP network addressing s
Directed Broadcasts.

IP Address Classes

Unique IP (Internet Protocol) addresses are assigned to each physical
if a device (host) has more than one connection to a network or networ

An IP address is represented as four decimal integers, with each integ
address is 32 bits long as per the following example:-

162.	146.	93.	14
10100010.	10010010.	01011101.	00001110

IP addresses are divided into two parts, a Network ID and a Host ID ea
always making 32 bits altogether.

Hint:- Use the Windows calculator to convert binary to decimal and vic

There are five primary classes of IP addresses and it is the high order
shown below:-

		First Octet	Example Network
Class A	0xxxxxxx	1-127	25.234.45.0
Class B	10xxxxxx	128-191	140.250.43.0
Class C	110xxxxx	192-223	192.2.3.0
Class D	1110xxxx	224-239	232.56.4.0

IP Addressing

Introduction

This section looks at IP addressing, subnet masking, Private and Special addresses. Examples are provided to illustrate the methodology when setting up an IP network addressing scheme. We also look at Wildcard masks and Directed Broadcasts.

IP Address Classes

Unique IP (Internet Protocol) addresses are assigned to each physical connection of a device to a network, therefore if a device (host) has more than one connection to a network or networks, then it will have more than one IP address.

An IP address is represented as four decimal integers, with each integer corresponding to one byte this means an IP address is 32 bits long as per the following example:-

```
162.      146.      93.       14        dotted decimal
10100010. 10010010. 01011101. 00001110  binary
```

IP addresses are divided into two parts, a Network ID and a Host ID each of which can be of varying bit lengths but always making 32 bits altogether.

Hint:- Use the Windows calculator to convert binary to decimal and vice versa.

There are five primary classes of IP addresses and it is the high order 3 bits of the address which identify the class as shown below:-

```
                First Octet    Example Network    Host
                1-127          25.234.45.0        1
Class A 0xxxxxxx
```

```
Class B 10xxxxxx    128-191    140.250.43.0    1
Class C 110xxxxx    192-223    192.2.3.0       1
Class D 1110xxxx    224-239    232.56.4.0      1
Class E 11110000    240-254    242.5.7.0       1
```

Class A addresses contain 7 bits in the network portion giving $2^7 - 2 = 126$ possible networks since all 1's and all 0's are not allowed. Consequently 24 bits remain for the host portion allowing a total of $2^{24} - 2 = 16,777,214$ hosts. **127.0.0.0/8** is reserved for loopback address purposes where just 127.0.0.1 is used normally. The address **255.255.255.255** is used as broadcast addresses and **0.0.0.0** as a default route address, meaning any network. The address 0.0.0.0 is sometimes used by hosts that have yet to receive an IP address e.g. a DHCP Client awaiting an address from the DHCP server.

Class B addresses contain 14 bits in the network portion allowing $2^{14} - 2 = 16,384$ possible networks, and 16 bits for the host portion allowing a possible total number of $2^{16} - 2 = 65,534$ hosts.

Class C addresses contain 21 bits for the network portion giving a possible total of $2^{21} - 2 = 2,097,152$ networks, and 8 bits for the host portion giving a possible $2^8 - 2 = 254$ hosts.

Class D addresses are used for multicasting and Class E addresses are used in research.

Historically, a company may have been allocated just one Class A, B or C IP address by the Network Information Centre (NIC). Currently, all Class A addresses have been allocated and most if not all of the Class B addresses have gone. If a company have a number of networks to manage then the network administrator may wish to subnet his network, that is create subnet addresses within the scope of the IP address that the administrator has been given.

Subnets

Subnetting Example

A customer has been given an IP address of 128.100.0.0 (a Class B address) for his company. He has specified that he requires 3 separate networks with the maximum possible number of host connections on each network.

The first two octets 128.100 are fixed since these are given by NIC as the Class B address, therefore we have the last

two octets to play with. Let us examine the possibilities more closely:

1. The address given

```
Octet 1     Octet 2     Octet 3     Octet 4
10000000    01100100    00000000    00000000
128.        100.        0.          0
```

2. We need to create a minimum of 3 different subnets but not at the expense of the number of host addresses available to us. The following process would seem to give us 4 permutations of subnets:
Looking at octet 3 specifically in binary, let us just use the first 2 bits for a subnet address:

```
128  64  32  16  8  4  2  1
1    1   0   0   0  0  0  0
```

The possible combinations for the first two bits are:

```
11   =   192   ->   128.100.192.0
10   =   128   ->   128.100.128.0
01   =   64    ->   128.100.64.0
00   =   0     ->   128.100.0.0
```

However all 1's and all 0's used to be not allowed for a subnet. These subnets are called the **All One's Subnet** and **Subnet Zero**. The reason for this was that older software found it difficult to distinguish between networks 128.100.0.0/16 and the all-zeros subnet 128.100.0.0/18. The same was true of the all-ones subnet. **RFC 950** therefore rules out '11' and '00' as useable subnets, we are therefore left with only two subnet addresses instead of the 3 we require.

3. Let us try and use an extra bit in octet 3:

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

The possible combinations are now:

```
111  =  224  ->  128.100.224.0
110  =  192  ->  128.100.192.0
101  =  160  ->  128.100.160.0
011  =  96   ->  128.100.96.0
001  =  32   ->  128.100.32.0
010  =  64   ->  128.100.64.0
100  =  128  ->  128.100.128.0
000  =  0    ->  128.100.0.0
```

As before all 1's and all 0's are not permitted for subnets, therefore we are left with 6 possible subnets (2^3 - 2):-

```
128.100.32.0
128.100.64.0
128.100.96.0
128.100.128.0
128.100.160.0
128.100.192.0
```

4. This leaves the rest of the bits (from power 16 downwards) in octet 3 and all the bits in octet 4 to construct the individual host addresses, the permutations amount to many thousands of hosts which should be plenty. Below is an example of a host address in subnet 128.100.192.0:-

```
128.100.194.23
```

On first inspection it would appear that address 128.100.194.23 has nothing to do with the subnet 128.100.192.0, so let us look a little more closely at the final two octets of the host address:

```
Octet 3 = 194
128  64  32  16   8   4   2   1
  1   1   0   0   0   0   1   0

Octet 4 = 23
128  64  32  16   8   4   2   1
  0   0   0   1   0   1   1   1
```

As we can see we are indeed part of the 128.100.192.0 subnet since it is only the first three bits of octet 3 which are used for the subnet address. All the bits from power 16 and downwards are allocated to the host address, so the power 2 bit just turns octet 3 from decimal 192 to decimal 194. Confusion frequently arises in this situation where the dividing line between the network portion of the IP address and the host portion rests part way through an octet (in this case between power 32 and power 16 of octet 3). Often it is possible to make the network/host dividing line between octets so that you can easily tell which host address belongs to which subnet.

Routers are used to minimise unnecessary traffic, and when running IP it is important to tell it which subnet an address is supposed to go. The way this is done, is at configuration by entering a 'subnet mask'.

The situation with the All-zeros and All-ones subnets nowadays is to allow them according to **RFC 1878**. This is because modern applications understand how to distinguish between these subnets and the main network.

Subnet masks

The subnet mask specifies the portion of the IP address that is going to be used for subnetworks (as opposed to hosts). For every bit position in the IP address that is part of the network ID or subnetwork ID, a '1' is set, and for every bit position in the IP address that is part of the host id portion, a '0' is set. The router uses the boolean AND operation with an incoming IP address to 'lose' the host portion of the IP address i.e. the bits that are '0', and match the network portion with its routing table. From this, the router can determine out of which interface to send the datagram. This means that the 'Don't care bits' are represented by binary 0's whilst the 'Do care bits' are represented by binary 1's.

For our example above, because we used the first three bits in octet 3 for our subnet addressing the subnet mask would be:

Octet 1	Octet 2	Octet 3	Octet 4

```
11111111    11111111    11100000    00000000
255.        255.        224.        0
```
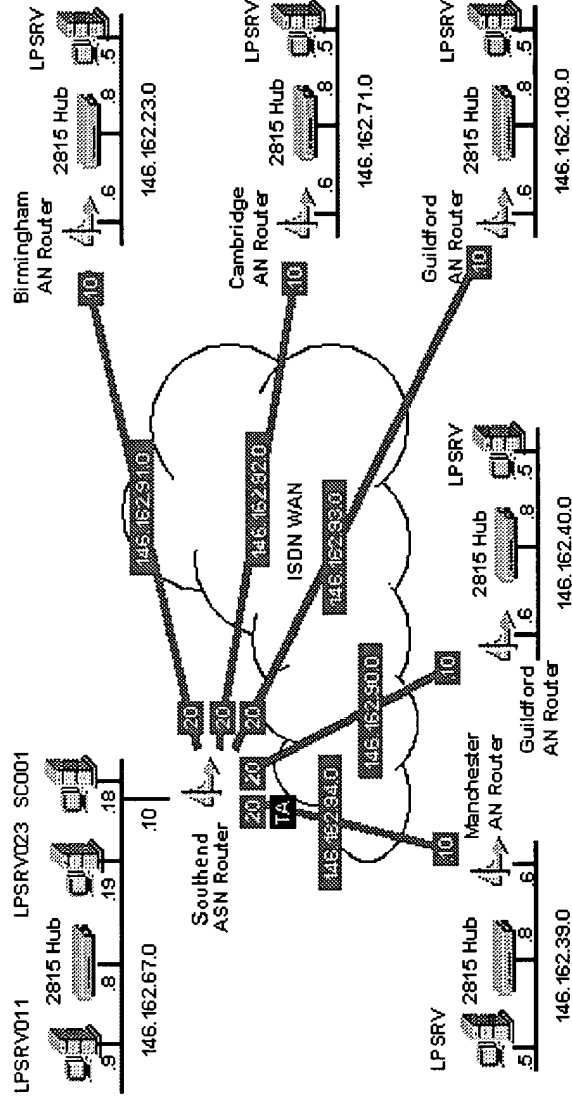
What is important is that the same mask is applied throughout the physical networks that share the same subnet part of the IP address. All devices connected to the networks that compose the subnet must have the same mask.

A **Broadcast Address** for a subnet is when all 1's are used in the host portion of the IP address. For example, for the IP address 10.17.20.4 and a mask of 255.255.255.0 the subnet is 10.17.20.0 and the host id is 4. The broadcast address within the 10.17.20.0 subnet is when the host id portion of the address is made up of all binary 1's. In this example the host portion is the last octet and if these 8 bits are set to 1 we have a broadcast address of 10.17.20.255. You can ping this, send messages to this and so on, a single line to server a multitude of end stations.

Often you will see the network mask represented as a number of bits e.g. for the above example address of 10.17.20.4 with a mask of 255.255.255.0, this can also be represented as 10.17.20.4/24, where the 24 represents 24 bits (3 octets) set to 1.

Another Subnetting Example

Study the schematic below:

IP Addressing, subnet mask, wildcard mask

LPSRV011 LPSRV023 SC001
2815 Hub
146.162.67.0
.9 .8 .5 .19 .18 .10

Southend
ASN Router

LPSRV
2815 Hub
146.162.39.0
.5 .8 .6

Manchester
AN Router

Birmingham
AN Router   LPSRV
2815 Hub
146.162.23.0
.10 .6 .8 .5

Cambridge
AN Router   LPSRV
2815 Hub
146.162.71.0
.10 .6 .8 .5

Guildford
AN Router   LPSRV
2815 Hub
146.162.103.0
.10 .6 .8 .5

Guildford
AN Router
2815 Hub
146.162.40.0
.6 .8 .5

ISDN WAN

.20

The network drawing above shows the IP address map for a WAN installation carried out for a large financial institution. The customer had installed 'Windows NT' servers at a number of sites and was requiring an ISDN link, star-wired out, from each of the sites from the main office server room. The IP addressing scheme had to take into account the following factors:-

• Up to 30 more sites may be added to the WAN in the near future.
• Each site could have up to 50 host connections.
• The customer had already assigned IP addresses to some of the servers and site PC's on the local LAN's.

The IP address given to this company was 146.162.0.0 (which is a Class B address), and the decision was made to use the whole of octet 3 for the subnet addresses leaving octet 4 for the host addresses. This made assigning IP addresses more easy to carry out and gave a maximum of 254 hosts per subnet and there could be a maximum of 254 subnets, thus satisfying the customer's requirements. The subnet mask for each subnet (Whether LAN or WAN) was consequently 255.255.255.0, it is important to design the addressing scheme such that the subnet mask is common to all LAN's/WAN's throughout the network unless a routing protocol such as OSPF is to be used. OSPF allows variable subnet masking.

9/17/04

Whilst studying the schematic you will note that the WAN links are 146.162.90.0 to 146.162.94.0 and the router ISDN interfaces are .20 at the main office end and .10 at the remote office end. Also you will note that the server IP addresses are all .5 and the ethernet hubs are all .8 while the router ethernet interfaces are all .6. Organising addressing like this can make life much easier especially when you are hopping from site to site.

RFC 950 and **RFC 1812** describes IP subnetting whereas **RFC 1009** defines Variable Length Subnet Masking.

Wildcard Masks

You will often come across Wildcard masks, particularly if you work with OSPF and/or Cisco routers. The use of wildcard masks is most prevalent when building Access Control Lists (ACLs) on Cisco routers. ACLs are filters and make use of wildcard masks to define the scope of the address filter. Although ACL wildcard masks are used with other protocols, we will concentrate on IP here.

Let us first take a simple example. We may want to filter a sub-network 10.1.1.0 which has a Class C mask (24-bit) 255.255.255.0. The ACL will require the scope of the addresses to be defined by a wildcard mask which, in this example is 0.0.0.255. This means that the 'Don't care bits' are represented by binary 1's whilst the 'Do care bits' are represented by binary 0's. You will note that this is the exact opposite to subnet masks!

Taking a more complex example. Say we wish to filter out a subnet which is given by 10.1.1.32 having a mask of 255.255.255.224. How do we find the wildcard mask for this? Well to help us, concentrating on the 4th octet, let us first look at the binary for this network and subnet mask. Then we reverse the binary bits to get the wildcard bits and then convert back to decimal to obtain the wildcard mask for the 4th octet:

4th octet in decimal	32
4th octet in binary	0 0 1 0 0 0 0 0
4th octet mask in decimal	224
4th octet mask in binary	1 1 1 0 0 0 0 0
Now the 4th octet wildcard in binary	0 0 0 1 1 1 1 1

Now the 4th octet wildcard in decimal | 31

The important bits have been highlighted in bold. The wildcard mask for the network 10.1.1.32/24 is 0.0.0.31.

The following table should help in seeing a pattern between the number of bits used for the mask in a particular octet, the subnet mask in decimal and the equivalent wildcard mask:

No. of Network Bits Set to 1	0	1	2	3	4	5	6	7	8
Subnet Mask Binary	00000000	10000000	11000000	11100000	11110000	11111000	11111100	11111110	11111111
Subnet Mask Decimal	0	128	192	224	240	248	252	254	255
Wildcard Mask Binary	11111111	01111111	00111111	00011111	00001111	00000111	00000011	00000001	00000000
Wildcard Mask	255	127	63	31	15	7	3	1	0

The binary for the wildcard mask is the exact reverse, bit for bit, of the subnet mask. You then calculate the decimal from the reversed binary bits to obtain the dotted decimal wildcard mask.

Private Addresses

One of the ways to combat the fast reduction in available IP address space was to introduce the concept of private

addresses and the use of Network Address Translator (NAT) to allow many organisations to use the same address space but not have this space visible on the Internet i.e. to use address translation on the edge of the networks.

The Class A network address range **10.0.0.0 to 10.255.255.255** (10.0.0.0/8) is designated for private use only. This address range cannot be used on the Internet as every ISP will automatically drop the address. This address is becoming very popular as its use in conjunction with **Network Address Translation (NAT)** has meant that large corporations can make use of the Class A address space available within 10.0.0.0 for their own private use internally and just use NAT for those relatively few addresses that do need to operate on the Internet. This is one reason why the immediate need for IP version 6 has been diminished.

There is also the private address range **172.16.0.0 to 172.31.255.255** (172.16.0.0/12) which is the CIDR block of 16 x Class B addresses 172.16.0.0, 172.17.0.0, ..., 172.31.0.0.

The network address range **192.168.0.0 to 192.168.255.255** (192.168.0.0/16) is also for private use and is a CIDR block of 256 x Class C addresses 192.168.0.0, 192.168.1.0, ..., 192.168.255.0.

Examine **RFC 1918** for more information on address allocation for private networks.

Other Special addresses

The address range **0.0.0.0/8** is currently considered throughout the Internet as for special use. Note that this is different from the host address 0.0.0.0/32 which means 'default'. You can have legitimate addresses in the range **0.0.0.0/16**, e.g. 0.0.123.95/16.

The address range **192.0.2.0/24** is called the **Test Net** and is reserved for use in testing examples and documentation.

The address range 169.254.0.0/16 is used for auto-configuration of IP addresses if a DHCP server should fail and there is no backup for the DHCP Clients. This is described in **RFC 2563** Stateless Auto-configuration.

Directed Broadcasts

The **RFC 1812** overviews the requirements of routers to run IPv4. One of the requirements is that routers MUST, by default accept Directed Broadcasts (although it is allowable to have a switch that turns this off). A directed broadcast is one where the IP broadcast has been sent to a destination prefix (a net or subnet). A directed broadcast destined for the network 10.20.20.0/24 would be 10.20.20.255, for example.

Masking IP Addresses

See **Masking IP Address** for information on hiding IP addresses.

Back to The IP Menu

Copyright © Rhys Haden 1998-2003